AFW

PATENT 2131

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: Dale E. Gulick Geoffrey S. Strongin	Examiner: B. Lanier
Serial No.: 09/853,443	Group Art Unit: 2131
Filed: May 11, 2001	Att'y Docket: 2000.039600
For: PROTECTION MECHANISM FOR BIOMETRIC INPUT DATA	Customer No. 023720

APPEAL BRIEF

CERTIFICATE OF MAILING
37 C.F.R. 1.8

I hereby certify that this correspondence is being deposited with the U.S. Postal Service with sufficient postage as First Class Mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on the date below:

07/28/05 Kathy Donas
Date Signature

Commissioner of Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Applicant hereby submits this Appeal Brief to the Board of Patent Appeals and Interferences in response to the final Office Action dated March 21, 2005. A Notice of Appeal was filed on June 17, 2005 and so this Appeal Brief is believed to be timely filed.

The Assistant Commissioner is authorized to deduct the fee for filing this Appeal Brief ($500) from **Advanced Micro Devices, Inc.'s Deposit Account 01-0365/TT3769**.[1]

08/03/2005 EFLORES 00000047 010365 09853443
01 FC:1402 500.00 DA

[1] In the event the monies in that account are insufficient, the Director is authorized to withdraw funds from Williams, Morgan & Amerson, P.C. Deposit Account No. 50-0786/2000.039600.

I. REAL PARTY IN INTEREST

The present application is owned by Advanced Micro Devices, Inc. The assignment of the present application to Advanced Micro Devices, Inc., is recorded at Reel 11804, Frame 0832.

II. RELATED APPEALS AND INTERFERENCES

Appellants are not aware of any related appeals and/or interferences that might affect the outcome of this proceeding.

III. STATUS OF THE CLAIMS

Claims 1-80 are pending in the application. Claims 1-2, 4, 7-12, 14-17, 20-24, 26, 28-32, 35-36, 38-47, 50-62, 65-66, 68-71, 73, and 75-80 stand finally rejected under 35 U.S.C. § 102(e) as allegedly being anticipated by Gennaro (U.S. Patent No. 6,317,834). Claims 25 and 72 stand finally rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Gennaro in view of Huang (U.S. Patent No. 5,856,789). The Examiner has provided no indication as to the disposition of claims 3, 5-6, 13, 18-19, 27, 33-34, 37, 48-49, 63-64, 67, and 74, so Appellants presume that these claims contain allowable subject matter.

IV. STATUS OF AMENDMENTS

There were no amendments after the final rejections.

V. SUMMARY OF CLAIMED SUBJECT MATTER

Independent claims 1, 14, 28, 58, and 75 set forth, among other things, a nonce. As defined in the specification and known to persons of ordinary skill in the art, a nonce is a number

generated to be used a single time to verify an identity. The nonce is typically a random number that links pairs of messages together for authentication purposes. Nonces may be used to overcome known vulnerabilities of passwords, in particular the fact that passwords are often used multiple times and therefore may be discovered by an unauthorized third party and used by the unauthorized third party. Nonces may also be used to help prevent replay attacks. See Patent Application, page 35, ll. 16-21. Independent claims 43 and 78 set forth, among other things, providing a random number, receiving biometric data, and authenticating the biometric data using the random number.

In one exemplary embodiment, a south bridge 330D and/or a processor 805F or other master device transmits a secret 4095 to each of the devices coupled to the master device capable of storing the secret 4095 at boot time or during some other trusted set-up. Thus, in the illustrated embodiment of Fig. 29A, the USB hub 4015, the biometric device 4020, and the smart card reader 4025 would each store the secret 4095. In other words, during the trusted set-up, the device or devices become known to the master device through an authentication routine, and the master device communicates the secret 4095 to those devices that authenticate properly as a trusted component of the computer subsystem 4000 or some part of the computer system. During data requests or transfers, the master device transmits a random number (or at least a nonce, a number that is used only once) to the device along with the data request. The device may encrypt the data using the random number (or the nonce) and the secret before transmitting the data to the master device. Whether or not the data is encrypted, the device returns the random number (or the nonce) with the data as an authenticator of the data.

As an example of this embodiment, consider the biometric device 4020 of Fig. 29A as a fingerprint scanner 4020. Placing a finger on the fingerprint scanner 4020 may cause the

fingerprint scanner 4020 to send an interrupt to the system. The fingerprint scanner 4020 scans the fingerprint of the finger on the fingerprint scanner 4020 to create fingerprint data. The system notifies the south bridge 330D, which sends the nonce to the fingerprint scanner 4020. The fingerprint scanner 4020 receives the nonce and returns the fingerprint data and the nonce to the south bridge 330D in response to receiving the nonce. The fingerprint scanner 4020 may also encrypt the fingerprint data using the nonce in lieu of sending the fingerprint data in the clear (*i.e.* not encrypted). See Patent Application, page 74, line 22 – page 75, line 20.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Appellant respectfully requests that the Board review and overturn the two rejections present in this case. The following issues are presented on appeal in this case:

(A) Whether claims 1-2, 4, 7-12, 14-17, 20-24, 26, 28-32, 35-36, 38-42, 58-62, 65-66, 68-71, 73, and 75-77 are anticipated by Gennaro;

(B) Whether claims 43-47, 50-57, and 78-80 are anticipated by Gennaro; and

(B) Whether claims 27 and 72 are obvious over Gennaro in view of Huang.

VII. ARGUMENT

A. Legal Standards

An anticipating reference by definition must disclose every limitation of the rejected claim in the same relationship to one another as set forth in the claim. *In re Bond*, 15 U.S.P.Q.2d 1566, 1567 (Fed. Cir. 1990).

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, the prior art reference (or references when combined) must teach or suggest all the claim limitations.

In re Royka, 490 F.2d 981, 180 U.S.P.Q. 580 (CCPA 1974). Second, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. That is, there must be something in the prior art as a whole to suggest the desirability, and thus the obviousness, of making the combination. *Panduit Corp. v. Dennison Mfg. Co.*, 810 F.2d 1561 (Fed. Cir. 1986). In fact, the absence of a suggestion to combine is dispositive in an obviousness determination. *Gambro Lundia AB v. Baxter Healthcare Corp.*, 110 F.3d 1573 (Fed. Cir. 1997). The mere fact that the prior art can be combined or modified does not make the resultant combination obvious unless the prior art also suggests the desirability of the combination. *In re Mills*, 916 F.2d 680, 16 U.S.P.Q.2d 1430 (Fed. Cir. 1990); M.P.E.P. § 2143.01. Third, there must be a reasonable expectation of success.

The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 U.S.P.Q.2d 1438 (Fed. Cir. 1991); M.P.E.P. § 2142. A recent Federal Circuit case emphasizes that, in an obviousness situation, the prior art must disclose each and every element of the claimed invention, and that any motivation to combine or modify the prior art must be based upon a suggestion in the prior art. *In re Lee*, 61 U.S.P.Q.2d 143 (Fed. Cir. 2002). Conclusory statements regarding common knowledge and common sense are insufficient to support a finding of obviousness. *Id.* at 1434-35.

It is by now well established that teaching away by the prior art constitutes *prima facie* evidence that the claimed invention is not obvious. *See, inter alia, In re Fine,* 5 U.S.P.Q.2d (BNA) 1596, 1599 (Fed. Cir. 1988); *In re Nielson*, 2 U.S.P.Q.2d (BNA) 1525, 1528 (Fed. Cir. 1987); *In re Hedges*, 228 U.S.P.Q. (BNA) 685, 687 (Fed. Cir. 1986).

B. Claims 1-2, 4, 7-12, 14-17, 20-24, 26, 28-32, 35-36, 38-42, 58-62, 65-66, 68-71, 73, and 75-77 Are Not Anticipated by Gennaro.

Gennaro describes capturing biometric information along with personal information unique to an individual. The biometric data may then be encrypted using a random encryption key, which may be generated from a password provided by the individual. However, Appellants respectfully submit that Gennaro fails to teach or suggest a nonce, as described above and set forth in independent claims 1, 14, 28, 58, and 75. The Examiner alleges that the limitations relied upon are not recited in the claims. Appellants respectfully disagree and note that Appellants may be their own lexicographer. In the present application, nonces have been defined in accordance with common usage in the art as a number generated to be used a single time to verify an identity. See Patent Application, page 35, ll. 16-21.

For at least the aforementioned reasons, Appellants respectfully submit that the present invention is not anticipated by Gennaro and request that the Examiner's rejections of claims 1-2, 4, 7-12, 14-17, 20-24, 26, 28-32, 35-36, 38-42, 58-62, 65-66, 68-71, 73, and 75-77 under 35 U.S.C. 102(e) be REVERSED.

C. Claims 43-47, 50-57, and 78-80 Are Not Anticipated by Gennaro.

Gennaro describes capturing biometric information along with personal information unique to an individual. The biometric data may then be encrypted using a random encryption key, which may be generated from a password provided by the individual. However, Appellants respectfully submit that Gennaro fails to teach or suggest authenticating biometric data using a random number, as set forth in independent claims 43 and 78. The Examiner alleges that

Gennaro describes using a random number to decrypt a stored biometric sample. However, Appellants submit that persons of ordinary skill in the art will appreciate that "decrypting" is not the same operation as "authenticating." In particular, decrypting refers to techniques that may be used to convert encrypted information back into its original form, whereas authentication refers to techniques for determining and/or verifying the identity of a user, a device, or another entity.

For at least the aforementioned reasons, Appellants respectfully submit that the present invention is not anticipated by Gennaro and request that the Examiner's rejections of claims 43-47, 50-57, and 78-80 under 35 U.S.C. 102(e) be REVERSED.

D. Claims 25 and 72 Are Not Obvious over Gennaro in view of Huang.

Claim 25 depends from independent claim 14. Claim 72 depends from independent claim 58. As discussed above, Gennaro fails to teach or suggest a nonce, as described above and set forth in independent claims 14 and 58. In rejecting claims 25 and 72, the Examiner relies upon Huang to teach a computer system containing a processor, a north bridge, and a south bridge. However, Huang also fails to teach or suggest a nonce.

The cited references also fail to provide any suggestion or motivation to modify the prior art to arrive at the claimed invention. To the contrary, Gennaro teaches away from the Examiner's proposed modification of the prior art. In particular, Gennaro teaches that the biometric data should be encrypted using a random encryption key generated based upon a password. As discussed above, nonces are used a single time, whereas passwords may be used multiple times and are therefore vulnerable to discovery by unauthorized third parties. Thus, teaching that biometric data should be encrypted based on a password teaches away from using a nonce.

For at least the aforementioned reasons, Appellants respectfully submit that the Examiner has failed to make a *prima facie* case that the present invention is obvious over Gennaro and Huang, either alone or in combination. Appellants request that the Examiner's rejection of claims 25 and 72 under 35 U.S.C. 103(a) be REVERSED.

VIII. CLAIMS APPENDIX

The claims that are the subject of the present appeal – claims 1-80 – are set forth in the attached "Claims Appendix."

IX. EVIDENCE APPENDIX

There is no separate Evidence Appendix for this appeal.

X. RELATED PROCEEDINGS APPENDIX

There is no Related Proceedings Appendix for this appeal.

XI. CONCLUSION

In view of the foregoing, it is respectfully submitted that the Examiner erred in not allowing all claims pending in the present application, claims 1-80, over the prior art of record. The undersigned may be contacted at (713) 934-4052 with respect to any questions, comments or suggestions relating to this appeal.

Respectfully submitted,

Date: 7/28/05

Mark W. Sincell, Ph.D.
Reg. No. 52,226
WILLIAMS, MORGAN & AMERSON
10333 Richmond, Suite 1100
Houston, Texas 77042
(713) 934-7000
(713) 934-7011 (facsimile)

AGENT FOR APPLICANTS

CLAIMS APPENDIX

1. (Original) A biometric device configured to receive a nonce, to receive biometric data, and to transmit the biometric data and the nonce.

2. (Original) The biometric device of claim 1 further configured to encrypt the biometric data using the nonce and to transmit only the encrypted biometric data and the nonce.

3. (Original) The biometric device of claim 1 further configured to receive a secret, to store the secret, and to transmit at least an indication of the secret with the biometric data.

4. (Previously Presented) The biometric device of claim 3 configured to encrypt the biometric data using the secret and to transmit only the encrypted biometric data and the nonce.

5. (Original) The biometric device of claim 4, further configured to encrypt the biometric data using the secret and the nonce.

6. (Previously Presented) The biometric device of claim 5 further configured with a globally unique identifier (GUID), wherein the biometric device is further configured to encrypt the biometric data using the GUID, the secret, and the nonce.

7. (Original) The biometric device of claim 3, wherein the secret comprises a system GUID.

8. (Original) The biometric device of claim 1, wherein the nonce further comprises a random number.

9. (Original) The biometric device of claim 1 further configured to receive the biometric data in response to receiving the nonce.

10. (Original) The biometric device of claim 9 further configured to receive the biometric data only in response to receiving the nonce.

11. (Original) The biometric device of claim 1, wherein the biometric data are taken from the group consisting of: a fingerprint or thumbprint, hand geometry, voiceprint, retinal scan, facial scan, body odor, ear shape, DNA profile, keystroke dynamics, pen stroke dynamics, and vein checking.

12. (Original) The biometric device of claim 1 further configured with a GUID, wherein the biometric device is further configured to encrypt the biometric data using the GUID and to transmit only the encrypted data and the nonce.

13. (Original) The biometric device of claim 12 further configured to encrypt the biometric data using the GUID and the nonce.

14. (Original) A computer system, comprising:

a biometric device configured to receive a nonce, to receive biometric data, and to transmit the biometric data and the nonce; and

a master device configured to provide the nonce to the biometric device and to receive the biometric data and the nonce from the biometric device.

15. (Original) The computer system of claim 14, wherein the biometric device is further configured to encrypt the biometric data using the nonce and to transmit only the encrypted biometric data and the nonce; and wherein the master device is further configured to receive the encrypted biometric data and the nonce from the biometric device and to decrypt the encrypted biometric data using the nonce.

16. (Original) The computer system of claim 14, wherein the biometric device is further configured to receive a secret, to store the secret, and to transmit at least an indication of the secret with the biometric data; and wherein the master device is further configured to receive at least the indication of the secret from the biometric device and to authenticate the biometric data as being from the biometric device using at least the indication of the secret.

17. (Previously Presented) The computer system of claim 16, wherein the biometric device is configured to encrypt the biometric data using the secret and to transmit only the encrypted biometric data and the nonce; and wherein the wherein the master device is further configured to receive the encrypted biometric data and the nonce from the biometric device and to decrypt the encrypted biometric data using the secret.

18. (Original) The computer system of claim 17, wherein the biometric device is further configured to encrypt the biometric data using the secret and the nonce; and wherein the master device is further configured to receive the encrypted biometric data and the nonce from the biometric device and to decrypt the encrypted biometric data using the secret and the nonce.

19. (Original) The computer system of claim 18, wherein the biometric device is further configured with a GUID, wherein the biometric device is further configured to encrypt the biometric data using the GUID, the secret, and the nonce.

20. (Original) The computer system of claim 16, wherein the secret comprises a system GUID.

21. (Original) The computer system of claim 14, wherein the nonce further comprises a random number.

22. (Original) The computer system of claim 22, wherein the biometric device is further configured to receive the biometric data in response to receiving the nonce.

23. (Original) The computer system of claim 16, wherein the biometric device is further configured to receive the biometric data only in response to receiving the nonce.

24. (Previously Presented) The computer system of claim 14, wherein the biometric data are taken from the group consisting of: a fingerprint or thumbprint, hand geometry, voice print, retinal scan, facial scan, body odor, ear shape, DNA profile, keystroke dynamics, pen stroke dynamics, and vein checking.

25. (Previously Presented) The computer system of claim 14, wherein the master device includes a processor, a north bridge, or a south bridge.

26. (Original) The computer system of claim 14, wherein the biometric device is further configured with a GUID, wherein the biometric device is further configured to encrypt the biometric data using the GUID and to transmit only the encrypted data and the nonce.

27. (Original) The computer system of claim 26 wherein the biometric device is further configured to encrypt the biometric data using the GUID and the nonce.

28. (Original) A method, comprising:

providing a nonce;

receiving biometric data; and

transmitting the biometric data and the nonce.

authenticating the biometric data using the nonce.

29. (Original) The method of claim 28, further comprising:

encrypting the biometric data;

wherein transmitting the biometric data and the nonce comprises transmitting only the encrypted biometric data and the nonce;

receiving the encrypted biometric data and the nonce; and

decrypting the encrypted biometric data.

30. (Original) The method of claim 29,

wherein encrypting the biometric data comprises encrypting the biometric data using the nonce; and

wherein decrypting the encrypted biometric data comprises decrypting the encrypted biometric data using the nonce.

31. (Original) The method of claim 29, further comprising:

receiving a secret;

storing the secret;

transmitting at least an indication of the secret with the biometric data;

receiving at least the indication of the secret; and

authenticating the biometric data using at least the indication of the secret.

32. (Original) The method of claim 31,

wherein encrypting the biometric data comprises encrypting the biometric data using the secret; and

wherein decrypting the encrypted biometric data comprises decrypting the encrypted biometric data using the secret.

33. (Original) The method of claim 32,

wherein encrypting the biometric data using the secret comprises encrypting the biometric data using the secret and the nonce; and

wherein decrypting the encrypted biometric data using the secret comprises decrypting the encrypted biometric data using the secret and the nonce.

34. (Original) The method of claim 33, further comprising:

providing a GUID;

wherein encrypting the biometric data using the secret and the nonce comprises encrypting the biometric data using the GUID, the secret, and the nonce; and

wherein decrypting the encrypted biometric data using the secret and the nonce comprises decrypting the encrypted biometric data using the GUID, the secret, and the nonce.

35. (Original) The method of claim 31, wherein the secret comprises a system GUID,

wherein receiving a secret comprises receiving the system GUID;

wherein storing the secret comprises storing the system GUID;

wherein transmitting at least the indication of the secret with the biometric data comprises transmitting at least the indication of the system GUID with the biometric data;

wherein receiving at least the indication of the secret comprises receiving at least the indication of the system GUID; and

wherein authenticating the biometric data using at least the indication of the secret comprises authenticating the biometric data using at least the indication of the system GUID.

36. (Original) The method of claim 35,

wherein encrypting the biometric data comprises encrypting the biometric data using the system GUID; and

wherein decrypting the encrypted biometric data comprises decrypting the encrypted biometric data using the system GUID.

37. (Original) The method of claim 36,

wherein encrypting the biometric data using the system GUID comprises encrypting the biometric data using the system GUID and the nonce; and

wherein decrypting the encrypted biometric data using the system GUID comprises decrypting the encrypted biometric data using the system GUID and the nonce.

38. (Original) The method of claim 28, further comprising:

receiving a secret;

storing the secret;

transmitting at least an indication of the secret with the biometric data;

receiving at least the indication of the secret; and

authenticating the biometric data using at least the indication of the secret.

39. (Original) The method of claim 28, wherein receiving the biometric data occurs in response to providing the nonce.

40. (Original) The method of claim 39, wherein receiving the biometric data occurs only in response to providing the nonce.

41. (Original) The method of claim 28, further comprising:

providing a GUID;

encrypting the biometric data using the GUID;

wherein transmitting the biometric data and the nonce comprises transmitting only the encrypted biometric data and the nonce;

receiving the encrypted biometric data and the nonce; and

decrypting the encrypted biometric data using the GUID.

42. (Original) The method of claim 41,

wherein encrypting the biometric data using the GUID comprises encrypting the biometric data using the GUID and the nonce; and

wherein decrypting the encrypted biometric data using the GUID comprises decrypting the encrypted biometric data using the GUID and the nonce.

43. (Original) A method, comprising:

providing a random number;

receiving biometric data; and

transmitting the biometric data and the random number.

authenticating the biometric data using the random number.

44. (Original) The method of claim 43, further comprising:

encrypting the biometric data;

wherein transmitting the biometric data and the random number comprises transmitting only the encrypted biometric data and the random number;

receiving the encrypted biometric data and the random number; and

decrypting the encrypted biometric data.

45. (Original) The method of claim 44,

wherein encrypting the biometric data comprises encrypting the biometric data using the random number; and

wherein decrypting the encrypted biometric data comprises decrypting the encrypted biometric data using the random number.

46. (Original) The method of claim 44, further comprising:

receiving a secret;

storing the secret;

transmitting at least an indication of the secret with the biometric data;

receiving at least the indication of the secret; and

authenticating the biometric data using at least the indication of the secret.

47. (Original) The method of claim 46,

wherein encrypting the biometric data comprises encrypting the biometric data using the secret; and

wherein decrypting the encrypted biometric data comprises decrypting the encrypted biometric data using the secret.

48. (Original) The method of claim 47,

wherein encrypting the biometric data using the secret comprises encrypting the biometric data using the secret and the random number; and

wherein decrypting the encrypted biometric data using the secret comprises decrypting the encrypted biometric data using the secret and the random number.

49. (Original) The method of claim 48, further comprising:

providing a GUID;

wherein encrypting the biometric data using the secret and the random number comprises encrypting the biometric data using the GUID, the secret, and the random number; and

wherein decrypting the encrypted biometric data using the secret and the random number comprises decrypting the encrypted biometric data using the GUID, the secret, and the random number.

50. (Original) The method of claim 46, wherein the secret comprises a system GUID,

wherein receiving a secret comprises receiving the system GUID;

wherein storing the secret comprises storing the system GUID;

wherein transmitting at least the indication of the secret with the biometric data comprises transmitting at least the indication of the system GUID with the biometric data;

wherein receiving at least the indication of the secret comprises receiving at least the indication of the system GUID; and

wherein authenticating the biometric data using at least the indication of the secret comprises authenticating the biometric data using at least the indication of the system GUID.

51. (Original) The method of claim 50,

wherein encrypting the biometric data comprises encrypting the biometric data using the system GUID; and

wherein decrypting the encrypted biometric data comprises decrypting the encrypted biometric data using the system GUID.

52. (Original) The method of claim 51,

wherein encrypting the biometric data using the system GUID comprises encrypting the biometric data using the system GUID and the random number; and

wherein decrypting the encrypted biometric data using the system GUID comprises decrypting the encrypted biometric data using the system GUID and the random number.

53. (Original) The method of claim 43, further comprising:

receiving a secret;

storing the secret;

transmitting at least an indication of the secret with the biometric data;

receiving at least the indication of the secret; and

authenticating the biometric data using at least the indication of the secret.

54. (Original) The method of claim 43, wherein receiving the biometric data occurs in response to providing the random number.

55. (Original) The method of claim 54, wherein receiving the biometric data occurs only in response to providing the random number.

56. (Original) The method of claim 43, further comprising:

providing a GUID;

encrypting the biometric data using the GUID;

wherein transmitting the biometric data and the random number comprises transmitting only the encrypted biometric data and the random number;

receiving the encrypted biometric data and the random number; and

decrypting the encrypted biometric data using the GUID.

57. (Original) The method of claim 56,

wherein encrypting the biometric data using the GUID comprises encrypting the biometric data using the GUID and the random number; and

wherein decrypting the encrypted biometric data using the GUID comprises decrypting the encrypted biometric data using the GUID and the random number.

58. (Original) A method for operating a computer system including a biometric device and a master device, the method comprising:

the master device providing a nonce;

the biometric device receiving biometric data; and

the biometric device transmitting the biometric data and the nonce to the master device.

59. (Original) The method of claim 58, further comprising:

the biometric device encrypting the biometric data;

wherein the biometric device transmitting the biometric data and the nonce to the master device comprises the biometric device transmitting only the encrypted biometric data and the nonce to the master device;

the master device receiving the encrypted biometric data and the nonce from the biometric device; and

the master device decrypting the encrypted biometric data.

60. (Original) The method of claim 59,

wherein the biometric device encrypting the biometric data comprises the biometric device encrypting the biometric data using the nonce; and

wherein the master device decrypting the encrypted biometric data comprises the master device decrypting the encrypted biometric data using the nonce.

61. (Original) The method of claim 59, further comprising:

the biometric device receiving a secret;

the biometric device storing the secret;

the biometric device transmitting at least an indication of the secret with the biometric data to the master device;

the master device receiving at least the indication of the secret from the biometric device; and

the master device authenticating the biometric data using at least the indication of the secret.

62. (Original) The method of claim 61,

wherein the biometric device encrypting the biometric data comprises the biometric device encrypting the biometric data using the secret; and

wherein the master device decrypting the encrypted biometric data comprises the master device decrypting the encrypted biometric data using the secret.

63. (Original) The method of claim 62,

wherein the biometric device encrypting the biometric data using the secret comprises the biometric device encrypting the biometric data using the secret and the nonce; and

wherein the master device decrypting the encrypted biometric data using the secret comprises the master device decrypting the encrypted biometric data using the secret and the nonce.

64. (Original) The method of claim 63, further comprising:

providing a GUID from the biometric device to the master device;

wherein the biometric device encrypting the biometric data using the secret and the nonce comprises the biometric device encrypting the biometric data using the GUID, the secret, and the nonce; and

wherein the master device decrypting the encrypted biometric data using the secret and the nonce comprises the master device decrypting the encrypted biometric data using the GUID, the secret, and the nonce.

65. (Original) The method of claim 61, wherein the secret comprises a system GUID,

wherein the biometric device receiving a secret comprises the biometric device receiving the system GUID;

wherein the biometric device storing the secret comprises the biometric device storing the system GUID;

wherein the biometric device transmitting at least the indication of the secret with the biometric data to the master device comprises the biometric device transmitting at least the indication of the system GUID with the biometric data to the master device;

wherein the master device receiving at least the indication of the secret from the biometric device comprises receiving at least the indication of the system GUID from the biometric device; and

wherein the master device authenticating the biometric data using at least the indication of the secret comprises the master device authenticating the biometric data using at least the indication of the system GUID.

66. (Original) The method of claim 65,

wherein the biometric device encrypting the biometric data comprises the biometric device encrypting the biometric data using the system GUID; and

wherein the master device decrypting the encrypted biometric data comprises the master device decrypting the encrypted biometric data using the system GUID.

67. (Original) The method of claim 66,

wherein the biometric device encrypting the biometric data using the system GUID comprises the biometric device encrypting the biometric data using the system GUID and the nonce; and

wherein the master device decrypting the encrypted biometric data using the system GUID comprises the master device decrypting the encrypted biometric data using the system GUID and the nonce.

68. (Original) The method of claim 58, further comprising:

the biometric device receiving a secret;

the biometric device storing the secret;

the biometric device transmitting at least an indication of the secret with the biometric data to the master device;

the master device receiving at least the indication of the secret from the biometric device; and

the master device authenticating the biometric data using at least the indication of the secret.

69. (Original) The method of claim 58, wherein the biometric device receiving the biometric data occurs in response to the master device providing the nonce to the biometric device.

70. (Original) The method of claim 69, wherein the biometric device receiving the biometric data occurs only in response to the master device providing the nonce to the biometric device.

71. (Original) The method of claim 58, wherein the biometric data are taken from the group consisting of: a fingerprint or thumbprint, hand geometry, voice print, retinal scan, facial scan, body odor, ear shape, DNA profile, keystroke dynamics, pen stroke dynamics, and vein checking, the method further comprising:

the master device providing the nonce;

the biometric device receiving the biometric data; and

the biometric device transmitting the biometric data and the nonce to the master device.

72. (Original) The method of claim 58, wherein the master device is selected from the group consisting of a processor, a bridge, a north bridge, a south bridge, and a motherboard, the method further comprising:

the master device providing the nonce;

the biometric device receiving the biometric data; and

the biometric device transmitting the biometric data and the nonce to the master device.

73. (Original) The method of claim 58, further comprising:

providing a GUID from the biometric device to the master device;

the biometric device encrypting the biometric data using the GUID;

wherein the biometric device transmitting the biometric data and the nonce to the master device comprises the biometric device transmitting only the encrypted biometric data and the nonce to the master device;

the master device receiving the encrypted biometric data and the nonce from the biometric device; and

the master device decrypting the encrypted biometric data using the GUID.

74. (Original) The method of claim 73,

wherein the biometric device encrypting the biometric data using the GUID comprises the biometric device encrypting the biometric data using the GUID and the nonce; and

wherein the master device decrypting the encrypted biometric data using the GUID comprises the master device decrypting the encrypted biometric data using the GUID and the nonce.

75. (Original) A system, comprising:

means for providing a nonce;

means for receiving biometric data; and

means for transmitting the biometric data and the nonce; and

means for authenticating the biometric data using the nonce.

76. (Original) The system of claim 75, further comprising:

means for encrypting the biometric data;

wherein the means for transmitting the biometric data and the nonce comprise means for transmitting only the encrypted biometric data and the nonce;

means for receiving the encrypted biometric data and the nonce; and

means for decrypting the encrypted biometric data.

77. (Original) The system of claim 76,

wherein the means for encrypting the biometric data comprise means for encrypting the biometric data using the nonce; and

wherein the means for decrypting the encrypted biometric data comprise means for decrypting the encrypted biometric data using the nonce.

78. (Original) A system, comprising:

means for providing a random number;

means for receiving biometric data; and

means for transmitting the biometric data and the random number; and

means for authenticating the biometric data using the random number.

79. (Original) The system of claim 78, further comprising:

means for encrypting the biometric data;

wherein the means for transmitting the biometric data and the random number comprise means for transmitting only the encrypted biometric data and the random number;

means for receiving the encrypted biometric data and the random number; and

means for decrypting the encrypted biometric data.

80. (Original) The system of claim 79,

wherein the means for encrypting the biometric data comprise means for encrypting the biometric data using the random number; and

wherein the means for decrypting the encrypted biometric data comprise means for decrypting the encrypted biometric data using the random number.